The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

10/22/2014

11/11/2014 - Updated

SUBJECT:

Vulnerability in Microsoft OLE Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft Windows products, excluding Server 2003. The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office file that contains an OLE object. The attack requires user interaction to succeed on Windows clients with a default configuration, as User Account Control (UAC) is enabled and a consent prompt is displayed. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

NOVEMBER 11 – UPDATED EXECUTIVE SUMMARY:

An additional vulnerability in OLE has been reported leveraging Microsoft Internet Explorer. This vulnerability could allow remote code execution if a user visits a specially crafted web page.

THREAT INTELLIGENCE:

Microsoft has reported that limited, targeted attacks have been observed attempting to exploit this vulnerability through Microsoft PowerPoint.

SYSTEM AFFECTED:

Windows Vista
Windows 7
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2

Windows 8
Windows 8.1
Windows RT
Windows RT 8.1

NOVEMBER 11 – UPDATED SYSTEM AFFECTED:

Windows Server 2003

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium government entities: **High**
Small government entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been publicly reported in Microsoft Windows. This vulnerability can be triggered by opening a specially crafted file, via email attachment, or through the web. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted file to a user. For this attack scenario to be successful, the user must be convinced to open the specially crafted file containing the malicious Object Linking and Embedding (OLE) object. All Microsoft Office file types, as well as many other third-party file types could contain a malicious OLE object.

In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted Microsoft Office file, such as a PowerPoint file, that is used in an attempt to exploit this vulnerability. In addition, compromised websites (and websites that accept or host user-provided content) could contain specially crafted content that could exploit this vulnerability. An attacker would have no method to force users to visit a malicious website. Instead, an attacker would have to persuade the targeted user to visit the website, typically by getting them to click a link that directs a web browser to the attacker-controlled website.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

***NOVEMBER 11 – UPDATED TECHNICAL SUMMARY*:**

An additional vulnerability has been privately reported in Microsoft Internet Explorer. This vulnerability can be triggered by visiting a specially crafted web page.

In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by getting them to open an attachment sent through email.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate workarounds provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

NOVEMBER 11 – UPDATED RECOMMENDATIONS:

The following actions should be taken:

- ***Apply appropriate updates provided by Microsoft to vulnerable systems immediately after appropriate testing.***

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/3010060

https://support.microsoft.com/kb/3010060

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6352

SecurityFocus:

http://www.securityfocus.com/bid/70690

NOVEMBER 11 – UPDATED REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS14-064